What if AI took care of traffic as well as driving?

While public discussion concentrates on the idea of autonomous driving as an added feature in a vehicle, could it turn out that the real advantage lies in interoperability?

Artificial intelligence (AI) is empowering what has arguably become one of the most important trends in the automotive industry: autonomous driving. Manufacturers are already equipping their entry-level vehicles with emergency braking, collision warning and blind spot monitoring, and offering other advanced driver assistance systems (ADAS) as options, such as autopilot, auto lane change, autopark and summon. Even when these ADAS still require a human in the loop, they are clearly pushing towards level 5 vehicle automation.

A fully automated vehicle has to operate safely in all circumstances. It needs to adapt to a changing environment, in which other elements are also moving. Typically, the AI in the vehicle allocates 'uncertainty areas' to other objects in the road depending on their possible movements. However, as the number of moving elements in that environment increases, the system begins to require a reduction in these 'uncertainty areas' to accommodate its own trajectory. In the absence of additional data, this can only be achieved on the basis of suppositions collected and encoded in rules used by algorithms, with the assumption of risks.

© THI-Carissma, *research on autonomous driving.*

Who sets these rules and programs the algorithms? How can anybody decide what risks are acceptable? There may be grounds here to decide on liability in cases of damage due to the system taking the wrong decision while following its program, rather than malfunctions where insurance companies could step in (in March 2017, the German Road Traffic Act was adapted to open the way for autonomous driving, and some manufacturers already contemplate facing this responsibility).

As traffic increases and the vehicle enters the uncertainty area of other moving elements, some level of interaction becomes necessary. In the same way as human drivers need to communicate and exchange signals by means of indicator lights or acoustic devices, such as the horn, autonomous vehicles need to gather information on the trajectories to be followed by other vehicles in order to reduce uncertainty. If no risks are acceptable at all, autonomous vehicles will not be able to operate in heavy traffic on their own. To reduce the uncertainty areas of other vehicles, the system needs to increase the amount of information it has on them. Thus, vehicles need to be connected and closely cooperate with each other, so that all of them can accommodate their own trajectories according to those of others.

Potential impacts and developments

As with all AI applications, autonomous vehicles require abundant data. Information external to the vehicle is crucial, as it needs to know the structure of the road and the presence of obstacles or other vehicles in its path. Internal information is also essential, as the vehicle needs to know its own status and the reliability of critical elements, such as brakes. Even if autonomous vehicles need to detect traditional signals and allocate uncertainty areas while sharing the public thoroughfare with non-autonomous vehicles, pedestrians and even animals, an efficient exchange of information with as many other vehicles as possible will greatly increase their safety, as well as their performance.

It follows that the more information the system can gather from other vehicles, the better (V2V). And this information can refer to the path other vehicles intend to take, as well as to their reliability. A path will be

Author: Andrés García Higuera, Scientific Foresight Unit (STOA)

PE 656.317 – December 2020

less reliable if a human driver is likely to be operating the controls to change the predefined trajectory, and it would also be useful to know the status of the steering system and brakes of that other vehicle. Road infrastructure such as signals can also be involved and coordinate with the flow of vehicles, knowing their intended trajectories (V2I). The autonomous vehicle thus becomes connected and operates as a part of its environment and traffic (V2X). Mostly sharing of operational information is contemplated for this, however privacy concerns still apply to specific questions, e.g. vehicle tracking and driver monitoring systems (DMS).

Intelligent transport systems (ITS) are a technological revolution in the transportation and automotive sector. The main goal of ITS is interconnecting all vehicles in a network so that safety and efficiency measures can be deployed in coordination. Besides, ITS can offer additional services. In fact, these technologies are evolving into an adaptation of the internet of things (IoT) to the automotive field, which is emerging as one of the most important technological trends for coming years.

Recent advances on smart vehicles and ITS give rise to the idea of the connected car as a central paradigm of new propositions aimed at introduction of collaborative systems and interoperability. In this context, many solutions for fleet control are already commercially available, whereas traffic optimisation is considered a realistic option for the near future. However, all these systems rely on information that is often internal to the vehicle and controlled by its manufacturer. For collaborative traffic to be really effective, AI systems in all vehicles need to be open to free exchange of internal data and connected to a global network.

Manufacturers tend to use proprietary systems to ensure their revenue from maintenance operations in their vehicles. However, while manufacturers may arguably have a claim to this maintenance revenue, the way in which some of them are limiting remote connection and the access to the information gathered by the vehicle and necessary for diagnosis and repair operations, constitutes a serious drawback to the development of new solutions for traffic control that aim for safer and more efficient vehicle circulation.

Anticipatory policy-making

For these new solutions on collaborative systems to work, it is necessary that all of the information concerning every vehicle is made available, e.g. through the on-board diagnostic (OBD) port. Most industrial vehicles already incorporate telematics systems such as smart tachographs (now compulsory) and others, to report on their status for fleet management and maintenance. Today, only limited specific legislation regarding automated mobility exists. However, seven big vehicle manufacturers have agreed on a standard protocol regarding basic parameters for fleet management systems. This protocol, identified as the fleet management system (FMS), is not backed by any European regulation and only allows for basic interoperability between management systems operating with vehicles from different manufacturers.

There is a growing new market for telematics solutions, some of which are already being developed by companies emerging in this sector. However, these solutions require access to diagnostic data through the OBD port without the restrictions set in place by some vehicle manufacturers. On the other hand, these may arguably have a legitimate right to include restrictions and they are also concerned about possible safety issues related to open access to vehicle data.

The maintenance sector (represented by associations such as EGEA) makes a claim for specific regulation on these issues. EGEA argues that manufacturers frequently set security gateways (SGW) restricting access to OBD vehicle information. This practice is contrary to Regulation (EC) No 595/2009 on type-approval of motor vehicles and engines and on access to vehicle repair and maintenance information, which specifies that 'unrestricted access to vehicle repair information' must be allowed at all times, and to related regulation (EU) No 2018/858, which makes specific reference to OBD systems, and even rules on how this must be done. According to the regulation, the OBD data has to be available **for reading** while the vehicle is in motion. This prevents tampering under these conditions, thus eliminating possible concerns related to vehicle safety. Restricting access to vehicle information results in a dominant position for manufacturers that is contrary to free competition and EU market rules. Facilitating remote access to this information would allow the transport industry to become more proficient by improving fleet management through predictive maintenance. It would also create the required conditions for the development of new solutions based on Big Data and AI that will make transport safer and more efficient. Enforcing the sector's compliance with existing regulations and extending its scope (e.g. to increase references to remote data access), will help create the proper conditions for this sector to develop and grow with new solutions and service companies.